Enhancement of Security in Cloud using Hybrid Encryption Technique

Himanshu narang
M.tech
DCRUST (Murthal)
Haryana

Kavita Rathi
Assistant Professor
DCRUST (Murthal)
Haryana

Abstract— Cloud computing is a model that delivers various set of services which a user can avail over the internet on rent basis. Nowadays, cloud computing has attained great prominence due to various reasons for instance, on demand resource sharing and online storage of data. However, security is one of the major task that hinder the growth of cloud computing. Due to this security issue, organizations are reluctant towards cloud computing despite of having various features. Hence, the major concern of this research work is to ensure cloud security. For this, a hybrid encryption system has been proposed that merges the accessibility of a public-key cryptosystem (using RSA) with the proficiency of a symmetric key cryptosystem (via AES). This hybrid technique is a two way secured data encryption system, which focusses on the matters related to user's privacy, authentication and accuracy. This hybrid algorithm offers more security along with authentication in comparison to other hybrid algorithm given in literature.

Keywords— Public-key cryptosystem; Symmetric key cryptosystem; RSA; AES.

I. INTRODUCTION

Cloud computing is a prominent technology that provides the flexibility of storing large amount of data storage and using different softwares on rent. Cloud computing facilitates many services such as software as a service (SaaS), platform as a service (PaaS) and infrastructure as a service (IaaS) [1]. Despite of many features of cloud computing, it has not been used exhaustively due to some loop holes concerning security [2]. Hence, to block these loop holes related to security, an integrated methodology is proposed in this paper. This involves utilization of two algorithms, asymmetric encryption-Rivest, Shamir and Adleman (RSA) and symmetric Key Standard-Advanced Encryption Standard (AES) to provide two way data encryption. As we know, in encryption a plain text is transformed into cipher (secret) text using a special key before transmission [3]. This key can be either public or private. However at receiver side, in decryption, this cipher text is then decoded in order to obtain the original message using a key. Many algorithms have been given in literature for the encryption and decryption so far [4-10]. Among them, the most efficient ones in terms of performance and response time are RSA and AES. AES algorithm is a Symmetric key algorithm, first introduced by Joan Deaman and Vincent Rijmen [9], offers high speed in both software and hardware implementation and can operate on data blocks of 128, 192 and 256 bits in 10 to 14 rounds. Size of the key determines the number of rounds depends. In this technique, a block of data is encrypted first in order to obtain the cipher. This cipher then goes through a number of rounds resulting a cipher text output. Major issue with this technique is key exchange problem.

Further RSA is used in hybrid encryption technique along with AES. RSA is an asymmetric encryption technique, first proposed in 1977 by Ron Rivest, Adi Shamir, and Leonard Adleman [10]. In RSA, message is encrypted using a public key and a private key is generated at the receiver side using secured database [11]. Due to this, hacker can get confused as the incorrect private key can although decrypt the data but that decrypted data is not an original message. [12]. Two different keys used makes this technique a slow and complex process.

The main objective of this is the integration of both techniques in order to obtain better cloud security. Here, the cipher generated by the AES can be considered as encrypted data. In order to secure this encrypted data (cipher) on the cloud, the private key (used to decrypt the cipher data) will be encrypted using the RSA algorithm.

This paper is organized as: Section II describes literature review of different cloud security algorithms. AES and RSA techniques are studied in Section III. Hybrid of the two algorithm along with its Implementation are done under proposed Solution in section IV followed by conclusion drawn.

II. LITERATURE REVIEW

Cloud computing has some unavoidable flaws like security of data, files system, backups, network traffic, host security. They have suggested a concept of digital signature with RSA algorithm, to encrypt the data while drifting it over the network. Thus, by this, dual problem of authentication and security is solved. The potency of their work is the framework proposed to address security and privacy issue.

Volker Fusenig and Ayush Sharma [2][13]: proposed a new approach called cloud networking which enumerate networking functionalities to cloud computing and thereby enabling flexible and dynamic placement of virtual resources crossing provider borders. This technique allows various kinds of optimization, e.g., reducing latency or network load. This paper brings out a security architecture that facilitates a user of cloud networking to prescribe security requirements and enforcing them in the cloud networking infrastructure.

As per DeyanChen and Hong Zhao [3] [14] from the consumers' perspective, the security issues in cloud computing are specially data security and privacy protection, which remain the prime inhibitor for adoption of cloud computing services. A crisp but all-round analysis on data security and privacy protection issues associated with cloud computing across all stages of data life cycle was proposed by them. They also suggested various schemes and polices like airavat etc to protect data. This system can prevent privacy leakage without authorization in MapReduce computing process. The lowness is that it just a theory, which depends on other schemes and policies for its implementation.

As per Eman M. Mohamed and Hatem S. Abdelkader [8] [15], Cloud computing involves repositioning of the application software and databases to the large data centres, where the management of the data and services may not be fully trustworthy. However, this unique feature led to many security challenges. To solve this problem, every cloud provider encrypts the data by using encryption algorithms. Thus, their paper investigates the basic problem of cloud computing data security. A data security model of cloud computing based on the study of the cloud architecture was proposed by them. They implemented software to enhance work in a data security model for cloud computing. Finally, for evaluation process they applied this software in the Amazon EC2 Micro instance.

G. Jai Arul Jose, C. Sajeev, and Dr. C. Suyambulingom [9] [16]: proposed to generate RSA Public keys and Private Keys for public and private access to overcome the problem of data security. To ensure flow of the cloud data securely, a Certificate Binary file is used inside control node configuration file. The control node sends data through Secure Socket Layer after certificate activation. Finally, AES algorithm is used for encryption .This unique combination makes this solution best to prevent different types of attacks. The upper hand of their work is strong data security against various attacks. The software automatically slows down the service in case if a user attempts to login falsely for many times and thereby stopping the account service for the particular user temporarily.

III. ALGORITHM USED

A. Advanced Encryption Standard (AES)

AES [9] encrypt data blocks of 128bit. It offers variable key length of 128, 192, 256 bits and can have 10, 12, 14 or more rounds depending upon the key size. This algorithm involves n-1 rounds of four stages and a last n^{th} round having only three stages starts as shown in Fig. 1. It starts with add round key stage and is applicable on both encryption and decryption but in case of decryption each and every stage of a round is the inverse of the stages in encryption. The four stages are described as:

i. Substitute bytes or Sub bytes
ii. Shift rows
iii. Mix Columns
iv. Add Round Key

Last n^{th} round simply does not contain Mix Columns stage. All rounds of the decryption algorithm are inverse of the encryption technique, and are given as:

i. Inverse Shift rows
ii. Inverse Substitute bytes
iii. Inverse Add Round Key
iv. Inverse Mix Columns

In case of decryption also, the n^{th} round abandons the Inverse Mix Columns stage.

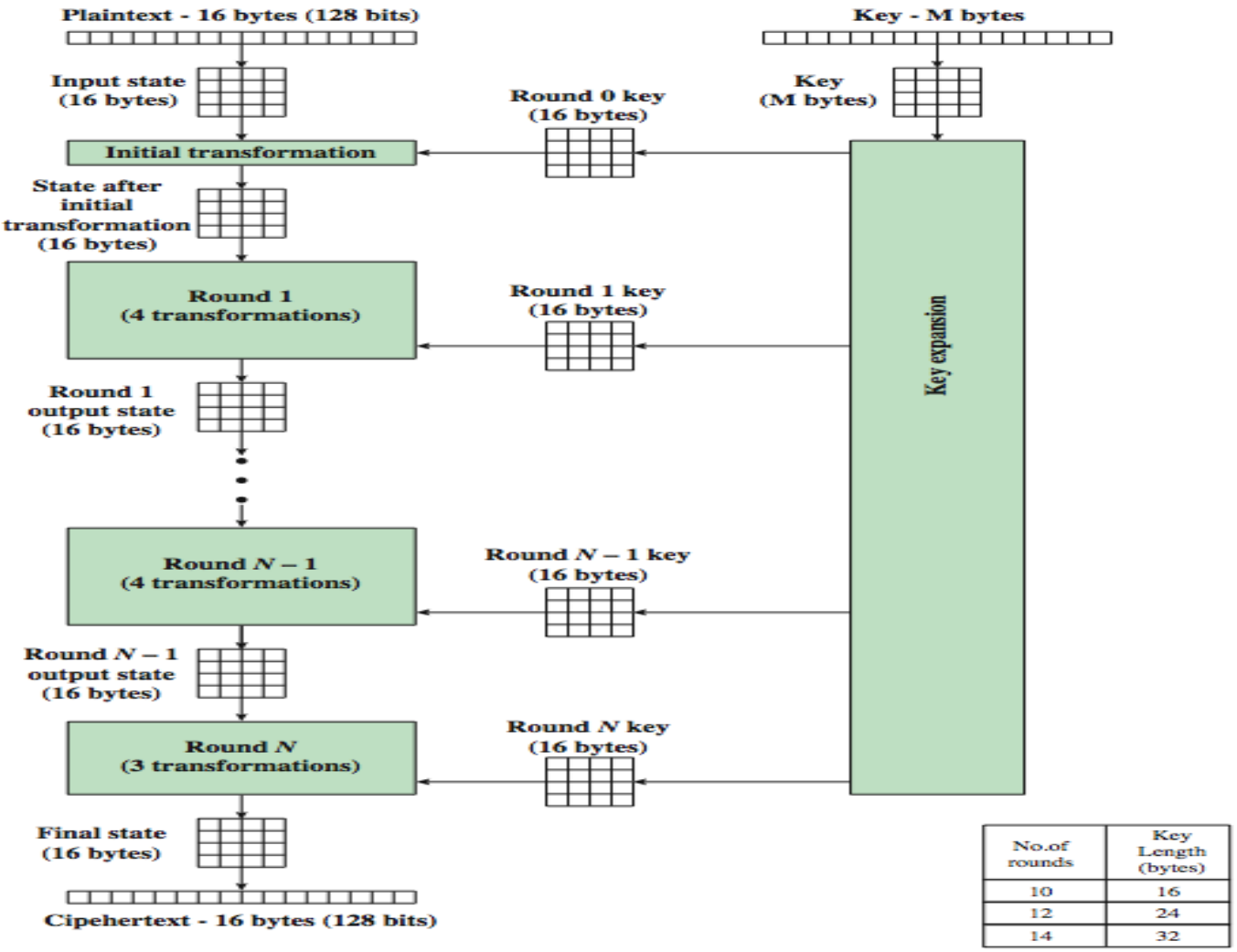

Fig. 1. AES Rounds

The detailed descriptions of all stages are given as:

i. Substitute bytes or Sub bytes

It consists of a well-defined lookup table formed with a 16×16 matrix of byte values called an s-box. For a certain round, each byte is transformed into a new byte. Left nibble of a byte denotes a specific row of s-box and the right nibble indicates a column. The matrix that gets operated upon throughout the encryption is known as state.

ii. Shift rows

In this state nth row is shifted to the left in circular manner by a factor n-1 as described below:

- The first row of state remains same.
- The second row is circularly shifted by one byte in the left.
- The third row is circularly shifted by two bytes in the left.
- The fourth row is circularly shifted by three bytes in the left.

One byte circular shift is equivalent to a linear shift of four bytes. This circular shift also confirms that the four bytes of one row are dispersed in four different columns.

iii. Mix Columns

This stage is also a substitution stage but it exploits arithmetic of GF (2^8). Every column is operated individually. Every byte of a column is converted into a new value which is a function of all the four bytes of that column.

iv. Add Round Key

In this stage, bits (128) of state are bitwise XORed with the bits (128) of the round key. The operation can be regarded as column wise operation among the 4 bytes of a \column of state and 1 word of the round key. This transformation should be simple to improve efficiency and also effects every bit of state.

Decryption is similar and done using inverse of all the encryption stages.

Advantage of AES:

1. Fast in hardware and software implementations.
2. Big size data encryption can be done.
3. Provisions for larger key size.
4. Less prone to attack.

Disadvantages of AES:

1. Key exchange is major issue as the same shared key is used for both encryption and decryption.
2. Prone to interpolation attack.

B. Rivest, Shamir and Adleman (RSA)

RSA is the widely used encryption algorithm for securing the data [10]. In RSA, key used to encrypt the data is public key which is different from the key used in decryption. Thus, the decryption key is secretly preserved. This asymmetry is constructed using the method of factoring the product of two large prime numbers. In this technique, both the plain text and cipher text are integers in between 0 and k-1 for some value k.
The plain text is encrypted in blocks, with each block having a binary value less than k. The public key in this technique consists of the *k* (which is termed as *modulus*) and *e* (referred as *public exponent*). The private key contains modulus *k* and *d* (known as *private exponent*) [17]. The public-key and private-key can be produced using the following steps:

1. Generate two random large prime's *p* and *q*.
2. Calculate modulus *k* as $k = p*q$.
3. Choose odd public exponent *e* in between 3 and *k*-1 which is relatively prime to *p*-1 and *q*-1.
4. Calculate private exponent *d* using *e*, *p* and *q*.
5. Output (*k*, *d*) as the private key and (*k*, *e*) as the public key.

The encryption in RSA is done as:

$$c = \text{encrypt}(t) = t^{e} \bmod k.$$

where *t* is the input *text* or *message*; the output *c* is the *cipher text*.
The decryption operation is described below:

$$m = \text{DECRYPT}(c) = c^{d} \bmod k.$$

The relationship between *e* and *d* is maintained in such a way that encryption and decryption are inverses. Hence, the original text or message *t* can be recovered easily from decryption operation. The private key (*k*, *d*) (or equivalently the prime factors *p* and *q*) is mandatory to recover *t* from *c*. Therefore, *k* and *e* can be easily made public without negotiating security.

Advantages of RSA:

1. Due to asymmetric key pair (private key and public key pair) no key exchange problem occurs.
2. Increased security and convenience.
3. Provides digital signatures that cannot be repudiated.

Limitations of RSA:

1. More memory is used
2. Large size data encryption cannot be done using RSA
3. Slow
4. Susceptible to impersonation attacks

IV. PROPOSED SOLUTION

A. Hybrid AES-RSA

As described in previous section, RSA cannot be operated on large size of data and AES has inherent key exchange issue. While transmitting data to cloud, we have to take in account a security solution that will overpower the limitations of both RSA and AES and will ensure data integrity simultaneously. The proposed solution is an integration of symmetric and asymmetric algorithm standards. This combination yields a hybrid algorithm that consists of essence of both AES and RSA. The hybrid encryption and decryption confirms that only genuine data will be traded between sender and receiver and this data cannot be altered [18]. When the plain text is encrypted by a user, it is first compressed as data compression spares modem transmission time, disk space and boosts cryptographic security. Most of the cryptanalysis techniques utilize patterns in the plain text to break the cipher. These patterns in the plaintext are degraded using compression, thereby improving resistance to cryptanalysis.

Then a secret key is generated, that is for one time only .This key is instance of AES Cipher class with the auto-generated secret key. This secret key then operates on conventional encryption algorithm in order to encrypt the plain text and results into a cipher text. When the data is encrypted, the secret key is then encrypted to form a recipient's public key. This public key (encrypted secret key) is then transmitted along with the cipher text to recipient.

Encryption Process:

The sender side encryption is shown in Fig. 2 and is explained as:

1. Generate an AES Secret Key (KAES) at runtime
2. Use AES encryption to encrypt the plain text data with KAES in order to obtain cipher text.
3. The key KAES is then encrypted using RSA algorithm with receiver's Public Key. The resulting cipher key is termed as ENCKAES.
4. Finally, prepare a file containing both cipher text and encrypted AES Secret key and send it to receiver.

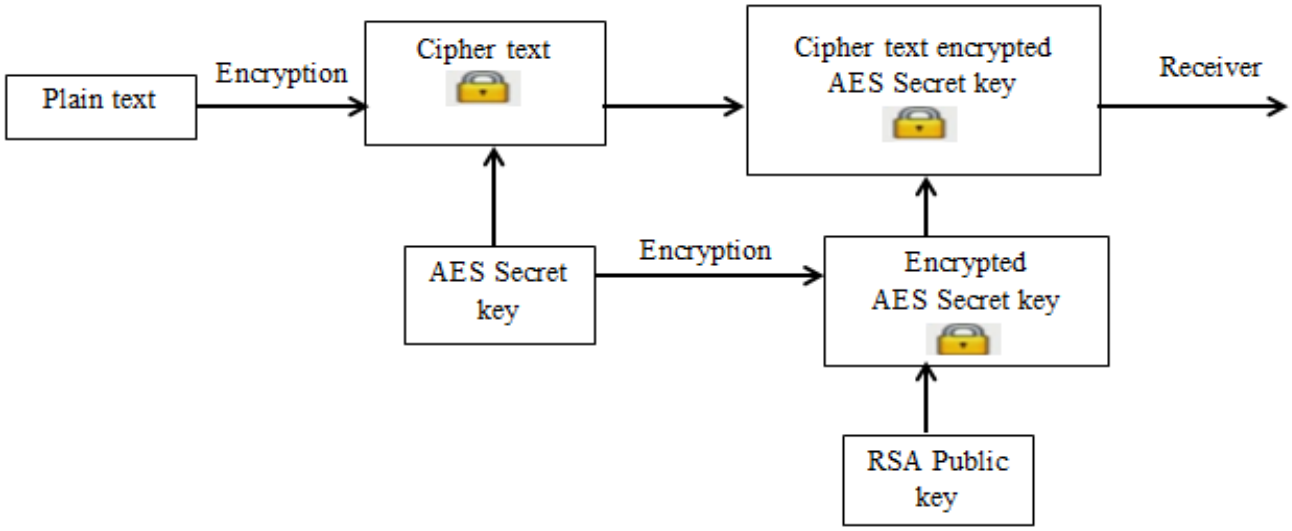

Fig. 2 Encryption of Proposed system

Decryption Process:

Decryption (given in Fig. 3) operates as just reverse of encryption. The recipient's copy of algorithm uses its private key to obtain the secret key, which is then used to decrypt the conventionally encrypted cipher text. The receiver side decryption terminology can be briefly summarized as below:

1. Process the received file and split out two components as encrypted cipher text and encrypted AES secret key.
2. RSA algorithm along with receiver's Private Key is used to decrypt the key ENCKAES. Cipher key is obtained which is same as AES secret key.
3. The cipher text is then decrypted using AES algorithm with AES Secret key and plain text is obtained.

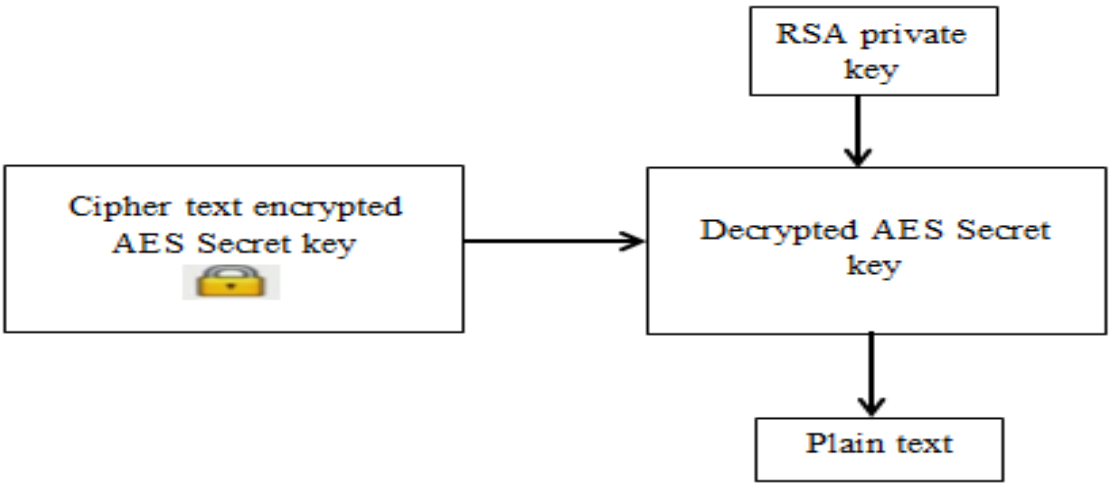

Fig. 3 Decryption of Proposed system

The hybrid of these two encryption method combines the convenience of public key encryption with the speed of conventional encryption. Public key encryption is very much slower than conventional encryption. However, public key encryption provides a way out to key distribution and data transmission issues. In this hybrid technique, performance and key distribution are improved without sacrificing security.

B. Implementation of Proposed technique

- *Software requirements*
  - ❖ Project platform – Java Operating
  - ❖ System – Windows 7
  - ❖ Cryptography Algorithms – RSA and AES
  - ❖ Protocol – TCP/IP
  - ❖ Software – Eclipse
  - ❖ Platform-CloudSim

  CloudSim: A new and simple extensible framework that allows flawless modelling, simulation and experimentation of developing Cloud computing infrastructures and applications. CloudSim can be of great use to researchers and industry-based developers to test the functioning of a newly developed application service in a controlled and easy to set-up environment.

- *Hardware Requirements*
  - ❖ Main – PENTIUM ¾
  - ❖ Processor RAM – 128MB
  - ❖ Hard disk – 4.2GB
  - ❖ Clock speed – 550 MHZ
  - ❖ System Bus speed – 400 MHZ
  - ❖ Cache RAM – 256 KB
- Results and Benefits of the Proposed Technique:

  1. High Security is obtained by using hybrid (RSA&AES) encryption algorithm.
  2. 1024 bit of RSA and 128 bit of AES keys are used, so one cannot predict the private key.

  Comparative study of AES, RSA and Hybrid AES-RSA is done as shown in fig.1.3 and is summarized in table-I as:

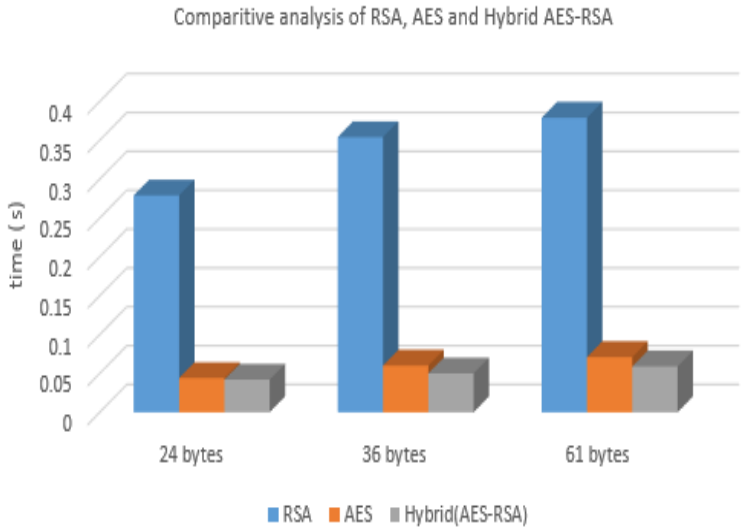

Fig. 4 Analysis of time required by different algorithm at different data size

Table-I Comparative analysis of AES, RSA and Hybrid AES-RSA

Input Data Size	RSA	AES	Hybrid(AES-RSA)
24 bytes	0.279s	0.044s	0.042s
36 bytes	0.354s	0.060s	0.050s
61 bytes	0.379s	0.071s	0.059s

V. CONCLUSION

The encryption and decryption of any data requires security of data as well as key. Due to this asymmetric key is used. The block cipher algorithm becomes more efficient with the use symmetric encryption technique. The outcome of the suggested research plan proves that processing time is very less in case of hybrid AES-RSA as compared to that of RSA and AES individually. Thus, AES algorithm along with RSA algorithm proves to be a capable technique in ensuring security of transmitted data. It is also presented that the proposed algorithm is better than any symmetric or asymmetric algorithm. Hence, recommended Hybrid Encryption Algorithm using Block cipher and symmetric key is found to be a more secure and convenient technique for secure data transmission in all kind of applications.

REFERENCES

[1] Wikipedia, http://en.wikipedia.org/wiki/Cloud Computing. cloud computing paper ref
[2] M. Zhou, R. Zhang, W.Xie, W. Qian& A.Zhou, “Security and privacy in cloud computing: A survey. In Semantics knowledge and grid (SKG)”, 2010 sixth international conference, **(2010)**; Beijing, China.
[3] D. Delfs., and K. Helmut, " Introduction To Cryptography: Principles and applications", Second Edition, Springer Science & Business Media, **(2007)**; Germany.
[4] K. Mehto, “A Secured and Searchable Encryption Algorithm for Cloud Storage,” vol. 120, no. 5, pp. 17–21, 2015.
[5] R. S and H. P. O H, “Biometric Based Approach for Data Sharing in Public Cloud,” *Ijarcce*, vol. 4, no. 2, pp. 95–97, 2015.
[6] A. I. Technology, H. Education, F. Women, H. Education, and F. Women, “ensuring security on mobile device data with two,” vol. 80, no. 2, pp. 221–226, 2015.
[7] F. Zhao, C. Li, F. Zhao, C. Li, and C.Feng Liu, “A cloud computing security solution based on fully homomorphic encryption,” pp. 485–488, 2014.
[8] C. Kant and Y. Sharma, "Enhanced Security Architecture for Cloud Data Security" International Journal of Advanced Research in Computer Science and Software Engineering, Volume 3, Issue 5, May 2013, pp. 571 -575.

[9] C. Wang, Q. Wang, K. Ren and W. Lou, "Ensuring Data Storage Security in Cloud Computing", In Quality of Service, 2009. 17th International Workshop on, page 19, 2009

[10] N.Y. Goshwe, Makurdi "Data Encryption and Decryption Using RSA Algorithm in a Network Environment" IJCSNS International Journal of Computer Science and Network Security, vol.13, no.7, (2013).

[11] R.S. Jamgekar, G. Shantanu Joshi, "File Encryption and Decryption Using Secure RSA", International Journal of Emerging Science and Engineering (IJESE), vol. 1, no. 4, **(2013)**.

[12] V. Fusenig and A. Sharma "Security Architecture for Cloud Networking" 2012 IEEE International Conference on Computing, Networking and Communications, Cloud Computing and Networking Symposium.

[13] D. Chen and H. Zhao "Data Security and Privacy Protection Issues in Cloud Computing" 2012 IEEE International Conference on Computer Science and Electronics Engineering

[14] Sherif el-etriby , E. Mohamed and H. Abdelkader published "Modern Encryption Techniques for Cloud Computing Randomness and Performance Testing " in the third international conference on communications and information technology ICCIT 2012

[15] G. Jai Arul Jose, C. Sajeev, Dr. C. Suyambulingom "Implementation of Data Security in Cloud Computing" International Journal of P2P Network Trends and Technology- Volume1 Issue1- 2011

[16] V. Kaul, S K Narayankhedkar, S Achrekar, S Agrawal, P Goyal, "Security Enhancement Algorithms for Data Transmission for Next Generation Networks", International Journal of Computer Application (IJCA).

[17] G. Singh, A. Singla, K. S. Sandha "Cryptography Algorithm Compaison For Security Enhancement In Wireless Intrusion Detection System" International Journal of Multidisciplinary Research Vol.1 Issue 4, August.

[18] K.W. Nafi, T.S. Kar, S.A. Hoque, M. M. A Hashem, "A Newer User Authentication, File encryption and Distributed Server Based Cloud Computing security architecture", International Journal of Advanced Computer Science and Applications, Vol. 3, No. 10, 2012.